system of Linehan as the claimed "security key manifest" which is a different basis of rejection supplied in the previous Office Action and is also inconsistent with the basis for rejection given, for example, on pages 3 and 4 of the instant final Action. As such, if the Patent Office has taken a position that the entire system of Linehan is the claimed security key manifest, Applicant respectfully submits that it does not appear to make technical sense since this would then also include the key client of Linehan which request a key and is no way part of any security key list or table. As such, Applicant is confused as to how this interpretation can anticipate Applicant's claimed invention. In addition, Applicant notes that a specific request was made for a showing as to which element in Linehan allegedly anticipates the structure and operation for dynamically controlling through a configured security key manifest, the generation of the new security key based on received key attribute data contained in the configured security key manifest. (previous response page 5). The final Action again does not provide specific structure or any cite to support showing of anticipation and Applicant respectfully requests another showing if the rejection is maintained.

In any event, for a reference to anticipate a claimed invention, the reference must teach each and every limitation in a manner in which it is claimed. Applicant respectfully submits that among other missing limitations, the Linehan reference does not teach:

> "dynamically controlling, through a configured security key manifest, the generation of at least one new security key for the subscriber based on <u>received key attribute data contained in</u> the configured security key manifest" (emphasis added)

Applicant respectfully submits that the Linehan reference does not, among other things, utilize any key attribute data that is contained within the configured security key manifest to dynamically control the generation of a new security key for a subscriber through the use of a configured security key manifest as required by the claims. For example, as noted in Applicant's specification, a subscriber may generate new security keys after evaluating a configured security key manifest that may be, for example, published in a repository by, for example, comparing key attribute data such as keys or other information with its own list of keys. Hence, received key attribute data contained in a configured security key manifest is used to dynamically control the generation of new security keys. Linehan does not operate in such a manner.

For example, the final Action states that the personal key database in Linehan acts as a security key manifest in that it contains an entry for each file that is to be accessed and each of the entries are indexed by information that identifies the files and each entry contains the key used to encrypt the corresponding file (final rejection page 3). However in Linehan, a new key is only generated once a key client of a creating user creates a data file and invokes the key generator to generate a key corresponding to the data file. The key generator then simply generates a key without comparing any other key attribute data in the file to any other information. Applicant respectfully requests a showing as to where the Linehan reference allegedly describes the generation of a new security key based on received key attribute data that is contained within the configured security key manifest as claimed. The Linehan reference teaches simply generating a new key upon each request from a key client without basing a key generation on any information contained within the personal key database. As such, the claims are in condition for allowance.

In addition, it appears that the final Office Action omits any comments or response to Applicant's previous arguments with respect to claim 15. As noted in the previous response, claim 15 more specifically requires that the subscriber compare the data security key manifest to preexisting credential sets that contain specific information such as, but not limited to, key size data, and key usage data and also requires that the subscriber update the preexisting credential set based on the comparison by generating at least one new key based on the content of the configurable key manifest. Linehan teaches an opposite approach in that the client does not do any key generation. Instead, Linehan requires that a separate personal key server generate the key and then send the key to the subscriber. Accordingly, Linehan teaches an opposite approach to that claimed by Applicant. These differences and combinations of the noted differences above are also believed to render this claim allowable.

With respect to claims 5, 35, 38 and 48, the Office Action alleges that Linehan teaches the claimed configured security key manifest in Col. 5, lines 9-16. However, Applicant respectfully notes that the cited portion of Linehan does not describe or relate to a configured security key manifest nor does it describe such a manifest including at least one of security key size, key usage, key maintenance attributes, cryptographic algorithm used, subscriber identification data and authentication data. To the contrary, the cited portion teaches merely that a client sends a ticket and data file identification to a server, namely, the key server and the key

server checks the ticket to verify that the accessing user is permitted to access the data file and then the key server sends the key corresponding to the data file to the client so that the client can decrypt the encrypted data file since it is the client that sends the ticket and data file identification data to the key server in Linehan. In contrast, Applicant claims that an already configured security key manifest includes updated data that is contained in the configured security key manifest, since the Office Action states as to claim 1 that the personal key data base of Linehan has been equated to the claimed configurable security key manifest of Applicant's claimed invention. However, the cited portion of Linehan indicates that a subscriber sends the identification ID to a key server. However, the personal key database of Linehan is already contained in the key server. Accordingly, these claims are also believed to be in condition for allowance.

As to claims 6, 10, 20 and 31, Applicant notes that these claims require, among other things, updating the preexisting credential set based on a comparison of preexisting credential sets containing at least one preexisting cryptographic security key. Applicant respectfully reasserts the relevant remarks made above.

Referring to claim 7, Applicant respectfully notes that the cited portion of Linehan merely teaches that the client or subscriber may generate a final encryption key. It is then sent to the personal key server at the time the file is created but notes that there is a disadvantage to this variance. In contrast, Applicant claims generating a new public key pair for the subscriber based on the contents of the configurable security key manifest. Applicant is unable to find reference to the generation of such a public key pair based on a configurable security key manifest as claimed. As noted above, the configurable security key manifest is a mechanism, such as a graphic user interface or other mechanism, that allows a security officer or other operator to configure the security key manifest to facilitate key generation. Such a system is not taught or suggested by Linehan.

As to claims 8, 18 and 29, this claim requires, among other things, continuously analyzing the configured security key manifest content, prior to using a security key pair to determine whether the suitable security key is necessary for a given operation. Such an operation is not described by Linehan.

With respect to claims 9, 19 and 30, Linehan is alleged to disclose encrypting a configurable key manifest with a key and userid, and validating the userid, in an authentication ticket against userid contained in the database, citing (Col. 16, lines 13-7). However, the claims require that the key manifest be digitally signed and it must be received and analyzed as claimed. The cited portion of Linehan refers to the encrypted file and not to a digitally signed key manifest.

Referring to claims 13, 23 and 34, Linehan has been cited as allegedly disclosing using symmetric data encryption keys that are stored in a configurable security key manifest. Applicant respectfully reasserts the relevant remarks made above with respect to claim 1 and submits that these claims are also in condition for allowance.

Referring to claims 27, 28, 42 and 43, the Applicant respectfully reasserts the relevant remarks made with respect to claim 25. Accordingly, these claims are also believed to be in condition for allowance.

Claims 4, 16, 37 and 47 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Linehan, in view of U.S. Publication No. 2001/0003828 (Peterson). These claims, require, among other things, issuing a configured key manifest for push based or pull based access by the subscriber, wherein the configurable security key manifest contains a non prespecified number of security keys and wherein a configured security key manifest dynamically controls the generation of a new security key for the subscriber based on received key attribute data contained in the configured security key manifest. Applicant respectfully reasserts the relevant remarks made above with respect to the Linehan reference and further notes that the Peterson reference is directed to a client side system for scheduling and delivering web content. The Office Action cites paragraph 46 of Peterson which merely indicates that a delivery of an index and web content can be done using pull based or push based architectures. Applicant respectfully submits that the Peterson reference does not appear to be directed to the problem faced by Applicant nor to the problem faced by Linehan and is not properly combinable with the Linehan reference since Peterson appears to be silent as to a method for creating security keys. As such, this combination of references cannot render Applicant's claim obvious.

Claims 11, 12, 17, 21, 22, 26, 32, 33, 41 and 45 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Linehan, in view of U.S. Patent No. 6,230,269 (Spies). Applicant respectfully reasserts the relevant remarks made above with respect to the Linehan reference and further notes that this claim requires a generation of key pairs and dynamically controlling the number of key pairs for a subscriber in response to the content of the configured security key manifest. As such, these claims are also believed to be in condition for allowance. Moreover, the cited portion of the Spies reference (Col. 1, lines 44-50) merely indicates that authentication is achieved through cryptographic public key systems. However, as noted above, none of the cited references describe using configurable key manifests and comparing key manifests to one another and using the key manifests to generate public keys. Accordingly, these claims are also believed to be in condition for allowance.

Accordingly, Applicant respectfully submits that the claims are in condition for allowance and that a timely Notice of Allowance be issued in this case. The Examiner is invited to contact the below-listed attorney if the Examiner believes that a telephone conference will advance the prosecution of this application.

Respectfully submitted,

By: _____
Christopher J. Reckamp
Registration No. 34,414

Date: March 28, 2003

Vedder, Price, Kaufman & Kammholz
222 N. LaSalle Street
Chicago, IL 60601
PHONE: (312) 609-7500
FAX: (312) 609-5005